

Ref. ③

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2002-26899

(P2002-26899A)

(43)公開日 平成14年1月25日(2002.1.25)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード*(参考)
H 0 4 L 9/32		G 0 9 C 1/00	6 4 0 D 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 B 7/24	E 5 K 0 3 3
H 0 4 B 7/24		H 0 4 L 9/00	6 7 5 B 5 K 0 6 7
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R
H 0 4 L 12/28		H 0 4 L 9/00	6 7 1

審査請求 有 請求項の数30 O L (全 14 頁) 最終頁に続く

(21)出願番号 特願2000-184697(P2000-184697)

(22)出願日 平成12年6月20日(2000.6.20)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSIN  
ESS MASCHINES CORPO  
RATION

アメリカ合衆国10504、ニューヨーク州

アーモンク (番地なし)

(74)復代理人 100085408

弁理士 山崎 隆 (外3名)

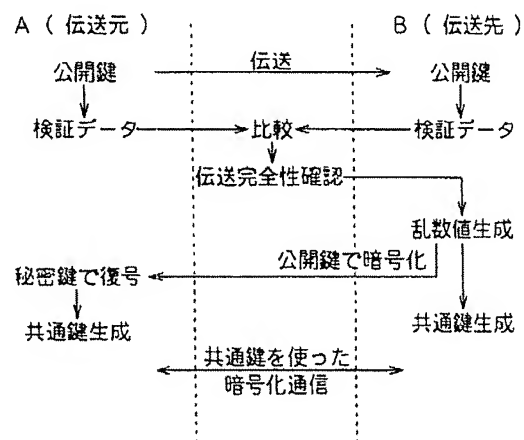
最終頁に続く

(54)【発明の名称】 アドホック無線通信用検証システム

(57)【要約】

【課題】 アドホック無線接続によるデータ送受信においてデータ完全性を簡単に検証する。

【解決手段】 暗号通信路開設を要求する要求元及び要求先をそれぞれ伝送元A及び伝送先Bと定義する。AとBとの間には、予め検証データ生成アルゴリズムID1が取り決められている。Aは、Bへ例えばAの公開鍵Kpを伝送するとともに、ID1によりKpから検証データXpを生成し、それを自分の検証画像表示部27へ出力する。Bは、AからKpとして伝送されて来たデータKxを受信し、ID1によりKxから検証データXxを生成し、それを自分の検証画像表示部27へ出力する。検証者は、A、Bの検証画像表示部27のXp、Xxが一致しているならば、データ完全性があると判断する。



## 【特許請求の範囲】

【請求項 1】 アドホック無線接続により相互に接続される 2 個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていないことを特徴とするアドホック無線通信用検証システム。

【請求項 2】 前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項 1 記載のアドホック無線通信用検証システム。

【請求項 3】 検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていないことを特徴とする請求項 1 記載のアドホック無線通信用検証システム。

【請求項 4】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を 1 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされることを特徴とする請求項 1～3 のいずれかに記載のアドホック無線通信用検証システム。

【請求項 5】 前記第 1 の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 1～3 のいずれかに記載のアドホック無線通信用検証システム。

【請求項 6】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を 2 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された 2 個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 5 記載のアドホック無線通信用検証システム。

【請求項 7】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそ

れぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 5 記載のアドホック無線通信用検証システム。

【請求項 8】 前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項 1～7 のいずれかに記載のアドホック無線通信用検証システム。

10 【請求項 9】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信用検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送されたことが検証されると、公開鍵 K p は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵 K c を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵 K c を第 2 の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵 K c に基づく暗号によりデータを送受することを特徴とする請求項 8 記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

30 【請求項 10】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信用検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵 K p が改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵 K c を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵 K c を第 2 の生成アルゴリズムから生成し、次に、共通鍵 K c は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵 K c に基づく暗号によりデータを送受することを特徴とする請求項 8 記載のアドホック無線通信用検証システムを利用するアドホック無線通信用データ送受システム。

50 【請求項 11】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在

し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、公開鍵  $K_p$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵  $K_p$  から共通鍵  $K_c$  を第 2 の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項 12】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、次に、共通鍵  $K_c$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受システム。

【請求項 13】 アドホック無線接続により相互に接続される 2 個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっていないことを特徴とするアドホック無線通信用検証方法。

【請求項 14】 前記検証データは、視覚的又は聴覚的な検証データであることを特徴とする請求項 13 記載のアドホック無線通信用検証方法。

【請求項 15】 検証データは検出データ出力部におい

て視覚的及び聴覚的の両方の出力形態で出力されるようになっていないことを特徴とする請求項 13 記載のアドホック無線通信用検証方法。

【請求項 16】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる方向性関数に係る演算子を 1 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされることを特徴とする請求項 13～15 のいずれかに記載のアドホック無線通信用検証方法。

【請求項 17】 前記第 1 の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 13～15 のいずれかに記載のアドホック無線通信用検証方法。

【請求項 18】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる方向性関数に係る演算子を 2 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された 2 個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 17 記載のアドホック無線通信用検証方法。

【請求項 19】 関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっていないことを特徴とする請求項 17 記載のアドホック無線通信用検証方法。

【請求項 20】 前記検証データ生成用データは一方のデータ送受装置の公開鍵であることを特徴とする請求項 13～19 のいずれかに記載のアドホック無線通信用検証方法。

【請求項 21】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、公

公開鍵  $K_p$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とする請求項 20 記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項 22】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、前記アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、次に、共通鍵  $K_c$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とする請求項 20 記載のアドホック無線通信用検証方法を利用するアドホック無線通信用データ送受方法。

【請求項 23】 各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、公開鍵  $K_p$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵  $K_p$  から共通鍵  $K_c$  を第 2 の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項 24】 各ユーザにより所有される無線通信機

能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵  $K_c$  を第 2 の生成アルゴリズムから生成し、次に、共通鍵  $K_c$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵  $K_c$  に基づく暗号によりデータを送受することを特徴とするアドホック無線通信用データ送受方法。

【請求項 25】 次の内容のアドホック無線通信用検証システム用プログラムを記録した記録媒体。

：アドホック無線接続により相互に接続される 2 個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【請求項 26】 次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項 25 記載の記録媒体。

：前記検証データは、視覚的又は聴覚的な検証データである。

【請求項 27】 次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項 25 記載の記録媒体。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【請求項 28】 次の内容のアドホック無線通信用検証システム用プログラムを記録した請求項 25 ～ 27 記載の記録媒体。

：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を 1 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【請求項 29】 次の内容のアドホック無線通信用検証

システム用プログラムを記録した請求項 25～27 記載の記録媒体。

：前記第 1 の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになってい

【請求項 30】 次の内容のアドホック無線通信用検証システム用プログラムを配信する配信装置。

：アドホック無線接続により相互に接続される 2 個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより前記第 1 の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになってい

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、伝送データの改ざんに対処するアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置に関するものである。

【0002】

【従来の技術】アドホック無線通信のような特定のインフラを利用しないその場限りの近距離無線通信において不特定の二者が、データを悪意の第三者により改ざんされることなく、伝送する場合には、悪意の第三者に知られることのない暗号鍵を共有する必要がある。しかしながら、通信時に随時その暗号鍵の基となる値を設定する方法は煩雑であり、特に通信相手が初顔合わせ等の状況下では、通信相手同士が口頭やメモ等により暗号鍵を交わすことはほとんど実用性がない。自動的に暗号鍵を共有する方法として、まず公開鍵を共有して、暗号鍵をその公開鍵で暗号化して共有する方法がある。しかし、マン・イン・ザ・ミドル・アタック (Man-in-the-middle attack : マン・イン・ザ・ミドル・アタックの詳細については、ジョン・ウィリィ・アンド・サンズ会社(John Wiley & Sons, Inc)出版の著者ブルース・シュナイアー (BRUCE SCHNEIER) の題名 : 応用暗号学 (APPLIED CRYPTOGRAPHY) の p. 48～p. 50 を参照されたい。) のリスクがある。

【0003】マン・イン・ザ・ミドル・アタックにおけるデータ改ざんのリスクを概略する。図 1 はアドホック無線通信システム 10 において送信元 A と送信先 B とが気付かないままに両者の間に悪意の第三者 C が介在する

余地を示している。A と B とは、(a) のように、両者間に直接、通信路が開設されていると、思っている、

(b) のように、実は第三者が両者の間に割り込んでいる場合がある。“Man-in-the-Middle Attack”がどのように実行されるのか、具体的に例を挙げて説明する。

【0004】無線暗号通信路開設の一般的な手順は以下のようになる。

手順 1 : 送信元は不特定多数の相手に向かって、通信したい送信先の ID で呼びかける。

手順 2 : 送信先が無線接続可能な範囲に居れば、その呼びかけられた ID (つまり自分の ID) を受信する。

手順 3 : 送信先は、自己の動作条件等を送信元に伝える。

手順 4 : 通信路開設のために必要な動作パラメータ (利用する通信路の選択と設定、暗号鍵の交換等) を両者で決定する。

手順 5 : 通信路開設し、相互通信が開始される。

【0005】悪意の第三者が図 1 の C の位置に最も入り込み易いのは、盗聴の対象となる二者が対面で無線通信を開始するタイミングである。つまり、上記の列挙された手順 1～3 に介入する。図 2 及び図 3 は悪意の第三者が図 1 の C の位置に入り込む手口の一例を示す。電波の性格上、送信元 A は周囲のすべての送信先候補に特定 ID で呼びかけざるを得ない (手順 1)。送信先 B は、自分の ID での呼びかけが聞こえるので (手順 2)、送信元 A に応答する (手順 3)。ここで、悪意の第三者は自分以外の ID への呼びかけに応答したり、自分以外の ID で呼びかけを行ったりして、下記のような成りすましを図ろうとする。まず、悪意の第三者 C は送信先 B の応答に同一周波数帯のノイズをぶつけて送信元 A がその応答を聞き取れないようにする。この時点で、送信先 B はそのノイズの事実を知らないで、上記手順 4 に移行して送信元 A からの手順 4 におけるセッション開始を待っている。送信元 A は手順 4 には居ないので、送信先 B はタイムアウト後に再度、自分の ID の呼びかけを聞く状態に戻る。一方、送信元 A は送信先 B からの応答が得られないので、タイムアウト後に再度同じ ID で呼びかける (手順 1) のが普通である。つまり、送信元 A と送信先 B は互いの手順の同期を取り始めようとして、それぞれのタイムアウトでその失敗に気がつき、元の状態に戻ることになる。

【0006】悪意の第三者 C は、送信元 A が再度同じ ID で呼びかけるタイミングに合わせて待機し、さらに送信先 B が再度自分の ID の呼びかけを聞き始めるタイミングにも合わせて待機する。以後、悪意の第三者 C は送信元 A の呼びかけに送信先 B に成りすまして応答し、反対に自分の ID の呼びかけを聞き始めた送信先 B に送信元 A に成りすまして呼びかけを行う。勿論、悪意の第三者 C はどのような ID にも自分の ID を変化させる能力を用意している。上記で送信元 A と送信先 B が互いの手

順の同期はずれから元の状態に戻るのとは同一時刻ではないので、このような二つの成りすまし行為を悪意の第三者Cは実行可能である。なぜなら、送信元Aと送信先Bがそれぞれ次のイベントで待機し始める時刻がそもそも異なるし、タイムアウトの対象となるイベントも異なるのでタイムアウト期間自身も異なるからである。

【0007】この成りすまし工作によって、送信元Aは、正規の送信先Bから正常な応答があったと思って、通信路開設手順、つまり手順4より悪意の第三者Cと一緒に遷移するし、送信先Bは、正規の送信元Aからの呼びかけだと思って、通信路開設手順に同じく第三者Cと一緒に遷移する。上記手順5まで進むと、二者のみで通信路を確保したと思っている両者A、Bの機器の保有者に知られることなく悪意の第三者Cが互いの間で通信データを中継する形で盗聴することが可能になる。この成りすまし（中継）を利用すれば、例えばAがBに送るはずの公開鍵をCが改ざんして、Cが予め用意した秘密鍵に対応した公開鍵とすり替えることができる。これによって、本来AとBの間に構築される暗号通信路はAとCの間でのみ有効になり、CとBとの間はCが別に設定した暗号通信路となる。つまり、Aから送られた暗号化データはCで復号化され、再度CとBの間の暗号化通信路用に別の暗号化を適用されて伝送される。その逆の伝送も同様である。AとBは共に通常手順で暗号化通信路を確立していながら、途中で公開鍵をすり替えられ、そのすり替えに気がつかないことで、盗聴される結果となる。このような攻撃（成りすましによる盗聴）をMan-in-the-middle attackと呼ぶ。暗号化通信路自身は安全であるから、このような攻撃への対処として、通信する両者で本当に同一の公開鍵を共有しているか否かを確実にすることが肝要となる。

【0008】

【発明が解決しようとする課題】Man-in-the-middle attackの対処法としては、認証機関の発行する証明書を利用して、証明書内に記載された個人ID（通常相手の名前等）を送元、伝送先で表示し目視比較することも考えられる。しかし、これには、証明書の発行にコストがかかる。また、認証機関を利用する場合、身元を登録して認証を行うため、通信相手に自分の身元を公開することになり、匿名性を保つことができないという問題も存在する。さらに、イエローページ（Yellow Page）のように公開鍵から利用者を特定するサービスを用いる場合は、電話回線等によるセキュアなネットワーク接続が必要であり、トランザクションコストがかかる。

【0009】本発明の目的は、アドホック無線接続により相互に接続されるデータ送受装置間でデータを送受する場合において、通信相手へのなりすましによるデータの改ざんを有効に防止できるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、

アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。本発明の他の目的は、口頭やメモ書きによるパスワードの取り交わしを省略でき、身元公開してしまう認証機関を利用せず、能率的に、円滑に、かつ正確に通信相手を検証することのできるアドホック無線通信用検証システム、アドホック無線通信用データ送受システム、アドホック無線通信用検証方法、アドホック無線通信用データ送受方法、並びに対応のプログラムを記録した及び配信する記録媒体及び配信装置を提供することである。

【0010】

【課題を解決するための手段】本発明のアドホック無線通信用検証システム及び方法によれば、アドホック無線接続により相互に接続される2個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【0011】両データ送受装置の距離は、両データ送受装置の検証データ出力部における検証データを相互に対比する必要があるため、典型的には、両データ送受装置間をユーザ（利用者）が数秒で行き来できる10m以内等であり、好ましくは数mである。検証データ生成用データに基づいて生成した検証データには検証データ生成用データそのものであってもよいとする。検証データは、両データ送受装置の検出データ出力部における検証データが相互に一致しているか否かの判定が行いやすいものに設定される。一般には、両データ送受装置において起動されている検証用ソフトが同一であれば、検証データ生成用データから検証データの生成のために同一の生成アルゴリズムが使用される。しかし、複数個の生成アルゴリズムの内の1個を、両データ送受装置のユーザがその場において適宜、取り決めたりするようになっているともよい。

【0012】一方のデータ送受装置は、送信した検証データ生成用データより第1の生成アルゴリズムに基づいて検証データを生成する。他方のデータ送受装置は、受信した検証データ生成用データより第1の生成アルゴリズムに基づいて検証データを生成する。そして、両データ送受装置の検出データ出力部から出力される検証データが一致するか否かの判定を行い、一致していれば、検証データ生成用データが、途中において改ざんされることなく、一方のデータ送受装置から他方のデータ送受装置へ正しく伝送されていること、すなわちデータ完全性

が検証されたことになる。このように、データ完全性の検証を能率的に実施できる。

【0013】本発明のアドホック無線通信用検証システム及び方法によれば、検証データは、視覚的又は聴覚的な検証データである。

【0014】視覚的な検証データには、画像、数値、文字、又はそれらの組み合わせがある。検証データの視覚表示の例としては、検証データが例えば計  $n$  ビットのビットデータである場合に、 $n$  ビットを、連続する等ビットずつで区分し、 $x$  軸方向へ区分、 $y$  軸方向へ各区分ごとの数量とするヒストグラムがある。検証データの聴覚表示の例としては、前述のヒストグラムの各区分の数量に対応する高さの音を、低位の区分から順番に出力するものである。検証データは、両データ送受装置における検証データの一致及び不一致をユーザが円滑かつ正確に判定し易いものが選択されるのが好ましい。

【0015】本発明のアドホック無線通信用検証システム及び方法によれば、検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっていること。

【0016】検証データの視覚的出力形態では、両データ送受装置におけるもの同士が類似していても、検証データの聴覚的出力形態では相違が明確であり、あるいはその逆の場合がある。検証データの視覚的出力形態及び聴覚的出力形態の両方が対比されることにより、一致及び不一致の判定の正確性が高まる。

【0017】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を 1 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【0018】一方向性関数には例えばハッシュ関数 (Hash Function) がある。上記定義した演算子列には、演算子が 1 個しかないものも含んでいる。検証データ生成用データからの検証データの生成に一方向性関数を関与させることにより、検証データから検証データ生成用データを見つけ出す困難性が増大し、悪意の第三者が真の検証データ生成用データに類似の偽の検証データ生成用データを使って、データ改ざんをする可能性が低下する。なお、検証データから検証データ生成用データを見つけ出すことは、直列演算子列の長さが長くなればなる程、計算量的に不可能となる。

【0019】本発明のアドホック無線通信用検証システム及び方法によれば、第 1 の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようにな

っている。

【0020】複数個の検証データ全部が類似している可能性は極めて低い。検証データを複数個、生成し、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されることにより、検証の正確性が向上する。

【0021】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を 2 個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列を構成する全演算子の中から選択された 2 個以上の演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【0022】本発明のアドホック無線通信用検証システム及び方法によれば、関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、相互に異なる一方向性関数に係る演算子を複数個、用意し、検証データ生成用データを各演算子の共通の入力とし、各演算子の出力又はその対応値をそれぞれ検証データとし、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【0023】本発明のアドホック無線通信用検証システム及び方法によれば、検証データ生成用データは一方のデータ送受装置の公開鍵である。

【0024】検証データ生成用データが一方のデータ送受装置の公開鍵であれば、検証データの検証により、他方のデータ送受装置が受信した公開鍵が一方のデータ送受装置の公開鍵であることを検証することができる。したがって、他方のデータ送受装置から一方のデータ送受装置へ一方のデータ送受装置の公開鍵を用いた暗号通信により例えば共通鍵等を送る等して、両データ送受装置間の共通鍵による暗号通信の開設を完全に実施できる。

【0025】前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵  $K_p$  が改ざんされることなく伝送されたことが検証されると、公開鍵  $K_p$  は各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、共通鍵  $K_c$  を第 2

の生成アルゴリズムから生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づく暗号によりデータを送受する。

【0026】前述のアドホック無線通信用検証システムを利用する本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、アドホック無線通信検証システムにより一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Kpが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Kcを第2の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、次に、共通鍵Kcは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づく暗号によりデータを送受する。

【0027】本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユーザの公開鍵Kpが改ざんされることなく伝送されたことが検証されると、公開鍵Kpは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、他方のユーザの無線通信機能付きパソコンは、公開鍵Kpから共通鍵Kcを第2の生成アルゴリズムに基づいて生成し、一方のユーザの無線通信機能付きパソコンは、他方のユーザの無線通信機能付きパソコンから公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づく暗号によりデータを送受する。

【0028】本発明のアドホック無線通信用データ送受システム及び方法によれば、各ユーザにより所有される無線通信機能付き携帯端末と無線通信機能付きパソコンとが存在し、各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとはセキュアな通信路で結ばれており、一方のユーザの無線通信機能付き携帯端末から他方のユーザの無線通信機能付き携帯端末へ一方のユー

ザの公開鍵Kpが改ざんされることなく伝送されたことが検証されると、他方のユーザの無線通信機能付き携帯端末は、共通鍵Kcを第2の生成アルゴリズムから生成し、一方のユーザの無線通信機能付き携帯端末は、他方のユーザの無線通信機能付き携帯端末から公開鍵による暗号を用いて伝送されて来た情報に基づいて共通鍵Kcを第2の生成アルゴリズムから生成し、次に、共通鍵Kcは各ユーザにおいて無線通信機能付き携帯端末から無線通信機能付きパソコンへ伝送され、両無線通信機能付きパソコンは、以降、共通鍵Kcに基づく暗号によりデータを送受する。

【0029】各ユーザの無線通信機能付き携帯端末と無線通信機能付きパソコンとのセキュアな通信路とは、例えば、各ユーザの秘密鍵による相互通信により確立される。無線通信機能付き携帯端末はPDA(Personal Digital Assistant)と呼ばれるものを含む。ビジネスマンの仕事のスタイルの一例としての隠しコンピューティング(Hidden Computing: 発明の実施の形態において詳述)が考えられている。隠しコンピューティングでは、例えばノートPC等の無線通信機能付きパソコン同士で、改ざんなくデータの送受が行われることが望まれる。このようなケースにおいて、ユーザは無線通信機能付き携帯端末の検証データ出力部における検証データの対比から一方の無線通信機能付き携帯端末の公開鍵Kpが途中で改ざんされることなく他方の無線通信機能付き携帯端末へ伝送されたことが検証されると、その検証を両ユーザの無線通信機能付きパソコンへ引き継がせ、両無線通信機能付きパソコンの間で共通鍵Kcにより暗号通信を円滑に実施できる。

【0030】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものである。  
：アドホック無線接続により相互に接続される2個のデータ送受装置の一方から他方へ検証データ生成用データを送り、一方のデータ送受装置では、送信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、また、他方のデータ送受装置では、受信した検証データ生成用データより第1の生成アルゴリズムに基づいて生成した検証データを自分の検証データ出力部に出力させ、両データ送受装置の検証データ出力部における検証データが相互に一致するか否かを判定されるようになっている。

【0031】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。録媒体。

：検証データは、視覚的又は聴覚的な検証データである。

【0032】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに

付加される。

：検証データは検出データ出力部において視覚的及び聴覚的の両方の出力形態で出力されるようになっている。

【0033】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

：関数を演算子、該演算子が作用する数値を該演算子の入力、該演算子の演算結果を該演算子の出力と定義し、同一又は異なる一方向性関数に係る演算子を1個以上、直列に並べた直列演算子列を設け、該直列演算子列の入力を検証データ生成用データとし、該直列演算子列の出力又はその対応値が検証データとされる。

【0034】本発明の記録媒体及び配信装置がそれぞれ記録及び配信するプログラムは次の内容のものがさらに付加される。

：第1の生成アルゴリズムは、検証データを複数個、生成するものであり、各検証データについて、両データ送受装置の検証データ出力部におけるもの同士が相互に一致するか否かを判定されるようになっている。

【0035】

【発明の実施の形態】以下、発明の実施の形態について図面を参照して説明する。図4はデータ完全性の検証及びそれに続く暗号データ伝送の全体のフローチャートである。暗号通信開設要求側及び被要求側をそれぞれ伝送元及び伝送先と定義し、図4では、伝送元データ送受装置をA、伝送先データ送受装置をBとしている。データ完全性検証のための公開鍵の伝送元及び伝送先と、データ完全性検証後の本伝送（ほんでんそう：共通鍵を使った暗号伝送）の伝送元及び伝送先とは、一致している必要はなく、逆であってもよいし、また、データ完全性検証後の本伝送では、伝送元及び伝送先は適宜、入れ替わってもよい。

【0036】図4の処理を順番に説明する。

(a) Aは、Bに暗号通信路開設要求と共に自分の公開鍵 $K_p$ 、及び検証データ生成アルゴリズムを指定するID（以下、このIDを「ID1」と言う。）を送信する。Aは、同時に、自分の公開鍵 $K_p$ を元に検証データ $X_p$ を生成する。

(b) BがAからAの公開鍵 $K_p$ として受信したデータを $K_x$ とする。もし、AからBへの無線伝送路においてデータの改ざんがなければ、 $K_x = K_p$ となり、改ざんがあれば、 $K_x$ は $K_p$ とは別のものとなる。BはAから受け取った $K_x$ を元に、Aより指定のあったID1の検証データ生成アルゴリズムで検証データ $X_x$ を生成する。検証データの例は、後述の図5において詳述する。

(c) A、Bのユーザは、A及びBの表示部にそれぞれ出力表示された検証データ $X_p$ 、 $X_x$ が同一であるか否かを検証する。もし、 $X_p = X_x$ であれば、 $K_x = K_p$ を意味し、A-Bの通信路にはデータ完全性があるとの判断を下す。

(d) BはAから受信した公開鍵 $K_p$ を使って、共通鍵生成のための乱数値 $R$ と共通鍵生成アルゴリズムを指定するID（以下、このIDを「ID2」と言う。）とを暗号化して、Aへ送信する。ID2については、A、Bが同一の通信ソフトを使用する等、ID2が固定されているならば、ID1と同様に、A-B間の伝送は省略できる。Bは、同時に乱数値 $R$ から共通鍵生成アルゴリズムを用いて共通鍵 $K_c$ を生成する。

(e) AはBから受信した暗号化された乱数値 $R$ を、公開鍵 $K_p$ に対応する秘密鍵を使って復号し、乱数値 $R$ とID2とを得、乱数値 $R$ からID2の共通鍵生成アルゴリズムを用いて共通鍵 $K_c$ を生成する。

(f) 以降、A-Bは、共通鍵 $K_c$ に基づく暗号化通信によりデータを送受する。

【0037】A、Bの検証データ出力部に表示する検証データは検証データ生成用データそのもの、例えばAの公開鍵そのものであってもよい。すなわち、A、Bの検証データ生成用データに、Aの公開鍵がビット表示される。しかし、数値では、読み取り難いので、公開鍵の数値表示を画像表示へ変換してもよい。図5は検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す。検証データはデータ送受装置20

(図6)の検証画像表示部27に視覚表示される。検証データ生成用データがAの公開鍵であるとして、公開鍵をLSBからMSBまでを等しいビット数の区域に順番に区切り、横軸を区域、縦軸を各区域の数量とするヒストグラムで、検証データが表されている。もし、Aの公開鍵 $K_p$ が、伝送路の途中で悪意の第三者により成りすましが行われていなければ、BがAより受信した検証データ生成用データ $K_x$ は、検証データ生成用データ $K_p$ に等しいので、 $X_x = X_p$ となる。したがって、A及び／又はBのユーザ、又は信頼できる他の検証者は、A、Bの表示部を直接、見て、A、Bの表示部に表示されている $X_p$ 及び $X_x$ を対比（比較）し、両者が一致していれば、AからBへAの公開鍵がそのまま伝送されて来たと判断し、すなわちデータ完全性があると判断し、両者が不一致であれば、AからBへの伝送途中にデータの改ざんがあったと判断する。

【0038】しかし、人間の認識能力の精度は必ずしも高くなく、図5のようなヒストグラムの比較画像を単純に生成しただけではハミングディスタンスの小さい類似公開鍵との違いを検出できない場合がある。そこで、公開鍵に対してハッシュ関数等の一方向性関数を適用して所定のデータへ変換し、それをヒストグラム等の検証画像の表示を行ってもよい。この場合、成りすましを行おうとする第三者が類似するデータを出力する別の公開鍵を求めようとしても、離散対数問題を解くことになり計算量的に不可能である。ただし、作成する検証画像の情報量が公開鍵のビットサイズに比べて極めて小さい場合、全数探索によって破られる可能性がある。そのよう

な条件下では、すでに方向性関数を適用したデータに対してさらに方向性関数を適用して新たなデータを算出したり、別の方向性関数を公開鍵に適用して新たなデータを算出したりして、別の検証画像を生成することができる。これを繰り返すことで、複数の検証画像を生成することができ、これを用いることで成りすましに対する強度をあげることができる。

【0039】検証データは、ヒストグラムのような画像に限定されず、文字データの表示や音階の変化などを用いたり、それらの複数のデータを組み合わせたりして、ユーザに対して提示したりしてもよい。聴覚的な検証データとしては、図5のヒストグラムの縦軸方向の値を音の高低又は音色に対応させ、図6の横軸方向の左の区域から順番に所定時間ごとに各区域の値に対応する音を出力する。また、検証データを視覚表示器と放音手段としてのスピーカとの両方から出力させるようにしてもよい。

【0040】図6～図8は方向性関数を使用して検証データ生成用データから検証データを生成する方式をそれぞれ示している。データD1は検証データ生成用データを意味し、データD2、D3、D4、・・・は検証データを意味する。また、各方向性関数は、演算子として機能し、入力に作用して、演算結果を出力する。方向性関数は例えばハッシュ関数(Hash Function)である。

【0041】図6では、1回目は検証データ生成用データとしてのデータD1に方向性関数Fを作用させ、データD2を得る。2回目は、データD2に同一の方向性関数Fを作用させ、すなわち、方向性関数Fを含むループを形成し、データD3を得る。以降、ループ処理を繰り返し、D4、D5、・・・を得る。所定回数のループを繰り返した後、最終的な演算結果をDnとし、このDnを検証データとし、この検証データをデータ送受装置20(図10)の検証画像表示部27に視覚表示する。最終的な演算結果Dnのみデータ送受装置20の検証画像表示部27に視覚表示するだけでなく、D2、D3、D4、・・・の特定の幾つか又は全部をデータ送受装置20の検証画像表示部27に画面分割又は時分割で視覚表示させることにし、表示されたそれぞれについて対比してもよい。複数の検証データを対比することにより、たとえそれらの1個の検証データについての一致・不一致の判定が紛らわしくても、対比される複数の検証データのすべてについて一致・不一致の判定が紛らわしくなる可能性は極めて小さく、データ改ざんについての検証の正確性を向上できる。

【0042】なお、D2、D3、D4、・・・の全部ではなく、特定の幾つかのみを対比する場合に、その幾つかについての組み合わせ(Subset)を適宜、変更するようにしておくことにより、悪意の第三者の攻撃に対する防護強度は高くなる。

【0043】図7では、相互に異なる複数の方向性関数F、G、H、・・・を用意し、共通のデータD1に各方向性関数F、G、H、・・・を作用させ、各演算結果D2、D3、D4、・・・を得る。D2、D3、D4、・・・の特定の幾つか又は全部を検証データとして、データ送受装置20の検証画像表示部27に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。

【0044】図8では、相互に異なる複数の方向性関数F、G、H、・・・を用意する。1回目は検証データ生成用データとしてのデータD1に方向性関数Fを作用させ、データD2を得る。2回目は、データD2に方向性関数Gを作用させ、データD3を得る。こうして、次々に前段の演算結果に次段の方向性関数を作用させ、複数のD2、D3、D4、・・・を得る。D2、D3、D4、・・・の特定の幾つか又は全部を検証データとして、データ送受装置20の検証画像表示部27に画面分割又は時分割で視覚表示させ、表示されたそれぞれについて対比する。なお、図6における複数の対比の方式は、図8の方式において、相互に異なる方向性関数を使用する代わりに同一の方向性関数Fを使用した特殊の例と考えることができる。

【0045】図9は図6～図8の処理を組み合わせる検証データを求める方式を示すブロック図である。図6～図9の検証データ演算方式をそれぞれタイプ(Type)1、2、3と定義している。図8の左端に検証データ生成用データが入力され、図8の右端に検証データが出力される。図9の配列例は一例である、タイプ1、2、3から2個以上のタイプを選択し、それらを任意の順に並べて、検証データ生成用データを得ることができる。

【0046】図10はデータ送受装置20のブロック図である。データ送受装置20は、場合により伝送元Aになったり、伝送先Bになったりするので、伝送元としての構成と伝送先としての構成を兼備している。データ送受装置20がAである場合には、伝送検証部24は、自分の公開鍵を検証画像生成部26へ出力し、また、データ送受装置20がBである場合には、通信部25においてAからの送受信データ31として受信したAの公開鍵は伝送検証部24を経由して検証画像生成部26へ送られる。検証画像生成部26は伝送検証部24から受けた公開鍵から検証データを生成し、生成された検証データは検証画像表示部27に表示される。A、Bの所有者等のユーザは、アドホック無線接続されている2個のデータ送受装置20の検証画像表示部27における検証データを対比し、一致及び不一致を調べ、その結果を検証結果入力部28に入力する。ユーザからの検証結果入力部28への入力結果は伝送検証部24へ通知され、伝送検証部24は、両検証データが相互に一致しているとの通知を受けた場合には、AからBへアドホック無線接続の伝

送路を介して伝送した公開鍵についてデータ完全性があると判断する。次に、データ送受装置 20 が B である場合には、乱数生成部 34 において乱数値が生成され、共通鍵生成部 33 では、乱数生成部 34 において生成された乱数値から ID2 の共通鍵生成アルゴリズムにより共通鍵を生成する。一方、乱数生成部 34 が生成した乱数値及び ID2 が復号化・暗号化実施部 32 において A の公開鍵に基づいて暗号化され、その暗号データ Dc が送受信データ 31 を介して A へ送られる。また、乱数値 R から ID2 の生成アルゴリズムに基づいて共通鍵を生成し、それを鍵保存部 35 に保存する。データ送受装置 20 が A である場合には、B から伝送されて来た暗号データ Dc の送受信データ 31 を復号化・暗号化実施部 32 において自分の秘密鍵により復号し、乱数値 R 及び ID2 を得、乱数値 R から ID2 の共通鍵生成アルゴリズムに基づいて共通鍵を生成し、該共通鍵を鍵保存部 35 に保存する。以降は、データを送信する場合は、鍵保存部 35 から共通鍵を引き出して、該共通鍵に基づいて送信データを復号化・暗号化実施部 32 において暗号化し、送受信データ 31 として相手方へ送信する。データを受信する場合は、受信した暗号化され送受信データ 31 を復号化・暗号化実施部 32 において復号し、平データをハードディスク（図示せず）等に保存したり、所定の処理を行ったりする。

【0047】図 11 は伝送元 A 側の通信処理のフローチャートである。公開鍵 Kp を送信し（S40）、該公開鍵 Kp から ID1 の検証データ生成アルゴリズムにより検証データ Xp を生成し（S42）、検証データ Xp を検証画像表示部 27 に出力する（S44）。S46 では、自分の検証データ Xp と伝送先 B の検証データ Xx とを対比して、同一と判断されれば、S48 へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、伝送先 B からの乱数値 R の受信を待ち（S48）、S50 において、乱数値 R を受信したと判断すると、S52 へ進み、乱数値受信待ち時間が所定時間経過したにもかかわらず、乱数値 R の受信のないときは、エラーとして該プログラムを終了する。S52 では、伝送先 B からの乱数値 R の暗号データを前記公開鍵 Kp に対応の自分の秘密鍵で復号して、乱数値 R を得る。A、B のデータ送受装置間では複数個の共通鍵生成アルゴリズムについてそれぞれ ID が予め取り決められており、送信先 B において今回の共通鍵生成アルゴリズムとして採用された ID（例では、ID2）が乱数値 R と一緒に伝送先 B から伝送元 A へ送信されて来ている。こうして、S56 では、乱数値 R から ID2 の共通鍵生成アルゴリズムに基づいて送信先 B との通信用の共通鍵を生成し、以降、該共通鍵を用いて B と暗号化通信を開始する（S58）。

【0048】図 12 は伝送先 B 側の通信処理のフロー

チャートである。伝送元 A から公開鍵 Kx を受信する（S60）。この受信した公開鍵は、A、B 間の伝送路に悪意の第三者が介在して改ざんされている可能性があるかもしれないので、Kc ではなく、Kx と表現することにする。次に、送信元 A から公開鍵 Kp と一緒に送られて来た ID1 で指定される検証データ生成アルゴリズムにより Kx から検証データ Xx を生成し（S62）、検証データ Xx を検証画像表示部 27 に出力する（S64）。S66 では、自分の検証データ Xx と伝送元 A の検証データ Xp とを対比して、同一と判断されれば、S68 へ進み、不一致と判断されれば、エラー（データ完全性が認められない）として、該プログラムを終了する。データ完全性がある場合には、乱数値 R を生成し（S68）、乱数値 R と、複数個の共通鍵生成アルゴリズムの中から、今回、選択した共通鍵生成アルゴリズムの ID としての ID2 とを送信元 A の公開鍵により暗号化したデータを送信元 A へ送信し（S70）、ID2 の共通鍵生成アルゴリズムに従って共通鍵 Kc を生成し（S72）、以降、該共通鍵を用いて A と暗号化通信を開始する（S74）。

【0049】図 13 は隠れコンピューティングスタイルの利用するユーザ間においてアドホック無線接続の暗号通信路を開設する説明図である。隠れコンピューティング（Hidden Computing）とは、ユーザは、コンピュータを鞆等に納め、手元の PDA（携帯情報端末：Personal Digital Assistant）等の携帯機器から無線通信等を利用して該コンピュータを遠隔操作する利用形態を意味する。PDA80a 等に装備されている 82 は通信デバイスである。上記に述べたような公開鍵のデータの完全性を確認できるシステムを装備していない機器（＝鞆 86a、86b 中のノートパソコン 88a、88b）間でアドホック無線通信を行う場合において、これらノートパソコン 88a、88b と事前にセキュアな通信路 90a、90b を確保している暗号通信路開設プロトコルを実装した PDA80a、80b を用いて、間接的に暗号通信路を開設する。なお、PDA とノートパソコンとの間のセキュアな通信路は、例えば両者間で事前に取り決められている共通鍵による暗号通信により達成される。図 13 においてまず手順（a）で通信路 84 を PDA80a、80b 間で開設して、一方の PDA の公開鍵を他方の PDA へ伝送して、該公開鍵のデータ完全性を検証する。次に、手順（b）において PDA80a、80b 間のデータ完全性検証を、それぞれの PDA80a、80b とセキュアな通信路 90a、90b により接続されているノートパソコン 88a、88b へ継承する。この継承は、具体的には、PDA80a、80b 間でデータ完全性を検証された公開鍵をセキュアな通信路 90a、90b を介してノートパソコン 88a、88b を伝送することにより達成される。以降、ノートパソコン 88a、88b は、両者間の

通信路 92 を介して共通鍵を共有した後、該共通鍵による暗号でデータを送受する。

【図面の簡単な説明】

【図 1】送信元 A と送信先 B とが気付かないまま両者の間に悪意の第三者 C が介入する余地を示す図である。

【図 2】悪意の第三者が図 1 の C の位置に入り込む手口の一例の第 1 の部分を示す図である。

【図 3】悪意の第三者が図 1 の C の位置に入り込む手口の一例の第 2 の部分を示す図である。

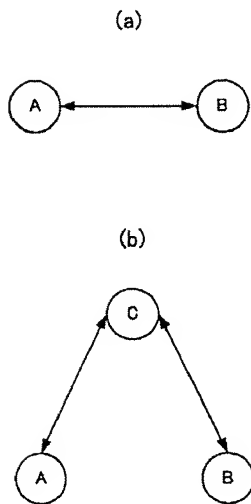
【図 4】データ完全性の検証及びそれに続く暗号データ 10 伝送の全体のフローチャートである。

【図 5】検証データ生成用データから生成した検証データの一例としてのヒストグラムを示す図である。

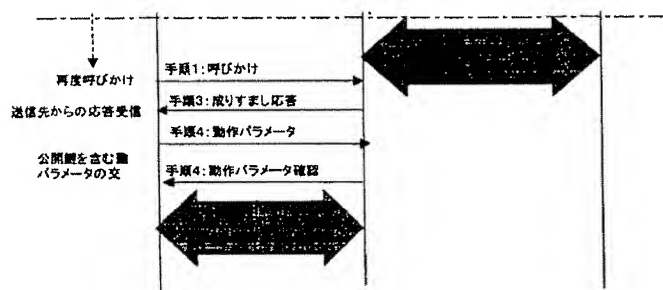
【図 6】一方向性関数を使用して検証データ生成用データから検証データを生成する第 1 の方式を示す図である。

【図 7】一方向性関数を使用して検証データ生成用データから検証データを生成する第 2 の方式を示す図である。

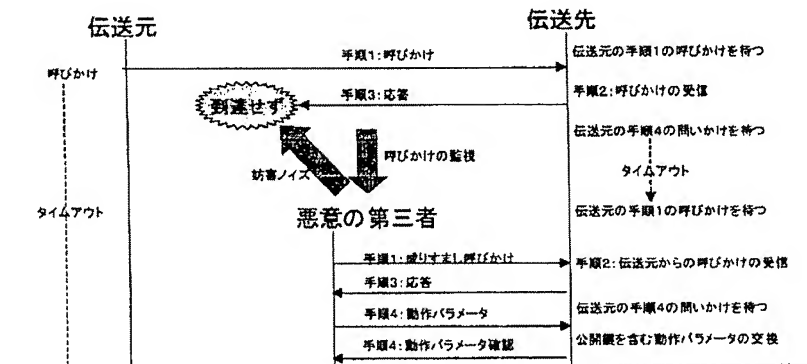
【図 1】



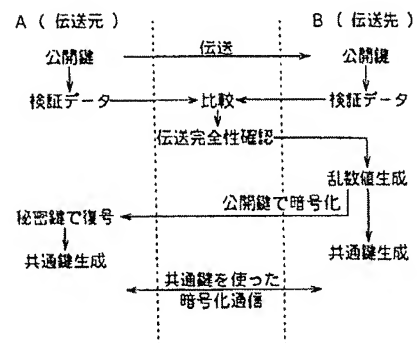
【図 3】



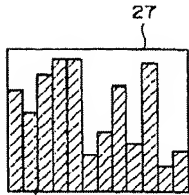
【図 2】



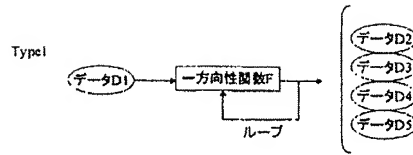
【図 4】



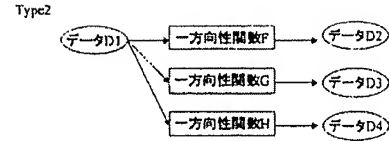
【図5】



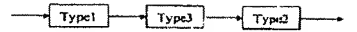
【図6】



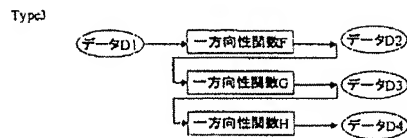
【図7】



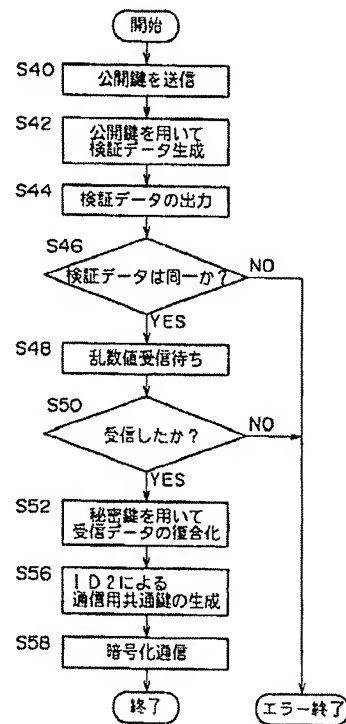
【図9】



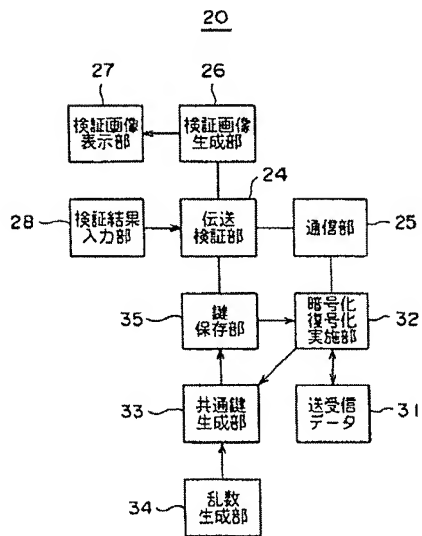
【図8】



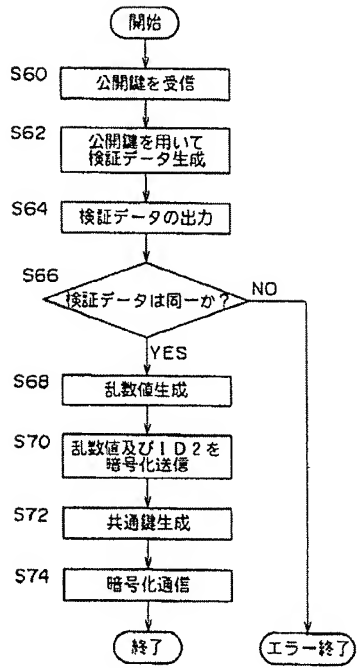
【図11】



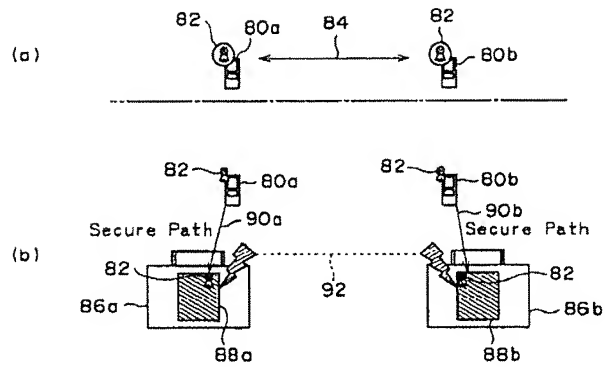
【図10】



【図 12】



【図 13】



フロントページの続き

(51) Int. Cl.<sup>7</sup>

識別記号

F I

7-コード (参考)

H 0 4 L 11/00

3 1 0 B

(72) 発明者 野口 哲也

神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

F ターム (参考) 5J104 AA07 AA08 AA16 AA41 EA04

EA10 EA19 JA21 JA29 KA01  
KA05 LA01 NA02 NA11 NA12  
NA24

(72) 発明者 下遠野 享

神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 東京基礎研究所  
内

5K033 AA08 BA08 DA17 DB20

5K067 AA33 BB04 BB21 DD17 DD53  
EE02 EE10 EE16 FF23 FF25  
HH22 HH23 HH36